IN THE CLAIMS:

The status of the claims is noted below:

1. (Currently Amended) A data processing apparatus comprising:

encrypting means for encrypting data in units of an encryption block having a predetermined data length;

processing means for ~~performing predetermined processing on said data in units of~~ defining a processing block having a data block length of a whole multiple of said predetermined length of said encryption block and for performing predetermined processing on data in units of said predetermined processing block length;

storage means for storing the encrypted data; and

control means for writing the encrypted data in said storage means so that the data positioned in the same encryption block is also positioned in the same processing block, said control means reading the data from said storage means in units of the processing block.

2. (Original) The data processing apparatus as set forth in claim 1, wherein said control means inserts data into said processing block to adjust the data length in the processing block so that the length of said processing block becomes a whole multiple of the predetermined data length of said encryption block.

3. (Original) The data processing apparatus as set forth in claim 1, wherein said encrypting means performs encryption processing using the encryption block to be encrypted and a cipher text obtained from the encryption of the encryption block immediately prior to the encryption block to be encrypted.

4. (Original) The data processing apparatus as set forth in claim 3, wherein said control means manages the encrypted data stored in said storage means using a cluster containing one or more processing blocks and values initially used when encrypting an encryption block in one of said processing blocks.

5. (Original) The data processing apparatus as set forth in claim 4, wherein said control means stores said one or more processing blocks at consecutive addresses of said storage means in

2

the order of encryption, stores said one or more encryption blocks in said processing blocks at consecutive addresses of said storage means in the order of encryption, and stores said initial values at an address immediately prior to the address of at which the first encryption block in the cluster is stored.

6. (Original) The data processing apparatus as set forth in claim 1, wherein said control means outputs said data read out in processing block units to said processing means.

7. (Original) The data processing apparatus as set forth in claim 6, wherein

said data is compressed; and

said processing means expands the data read from said storage means in units of a processing block.

8. (Currently Amended) A data processing system for inputting and outputting data while performing mutual identification between a storage apparatus and a data processing apparatus, said storage apparatus comprising:

first mutual identification processing means for performing processing for mutual identification with said data processing apparatus;

storage means for storing said data; and

first control means for allowing the input and output of data between said data processing apparatus and said storage means when said data processing apparatus is recognized to be a legitimate party by the processing for mutual identification;

said data processing apparatus comprising:

second mutual identification processing means for performing processing for mutual identification with said storage apparatus;

encrypting means for encrypting data in units of an encryption block of a predetermined data length;

processing means for defining ~~performing predetermined processing on said data in units of~~ a processing block having a data block length that is a whole multiple of the predetermined data

3

length of the encryption block ~~and for performing predetermined processing on data in units of said predetermined processing block length~~; and

second control means for performing at least one of write processing and read processing when said data processing apparatus is recognized to be a legitimate party by the processing for mutual identification, for writing the encrypted data in said storage means so that data positioned in one encryption block is also positioned in the same processing block during write processing, and for reading the data from said storage means in units of a processing block during read processing.

9. (Original) The data processing system as set forth in claim 8, wherein said second control means inserts data into said processing block to adjust the data length in the processing block so that the length of said processing block becomes a whole multiple of the predetermined data length of said encryption block.

10. (Original) The data processing system as set forth in claim 8, wherein said encrypting means performs encryption processing using the encryption block to be encrypted and a cipher text obtained from the encryption of the encryption block immediately prior to the encryption block to be encrypted.

11. (Original) The data processing system as set forth in claim 10, wherein said second control means manages the encrypted data stored in said storage means using a cluster containing one or more processing blocks and values initially used when encrypting an encryption block in one of said processing blocks.

12. (Original) The data processing system as set forth in claim 11, wherein the second control means stores said one or more processing blocks at consecutive addresses of said storage means in the order of encryption, stores said one or more encryption blocks in said processing blocks at consecutive addresses of said storage means in the order of encryption, and stores said initial values at an address immediately prior to the address of at which the first encryption block in the cluster is stored.

13. (Currently Amended) A data processing method, comprising the steps of:
encrypting data in units of an encryption block having a predetermined data length;

4

defining ~~performing predetermined processing on said data in units of~~ a processing block having a data block length that is a whole multiple of the predetermined data length of the encryption block;

~~performing predetermined processing on data in units of said predetermined processing block length;~~

writing the encrypted data to a storage means so that all of the data positioned in one encryption block is also positioned in the same processing block; and

reading the data from the storage means in units of the processing block.

14. (Original) The data processing method as set forth in claim 13, further comprising the step of inserting data into said processing block to adjust the data length in the processing block so that the length of said processing block becomes a whole multiple of the predetermined data length of said encryption block.

15. (Original) The data processing method as set forth in claim 13, further comprising the step of using the encryption block to be encrypted and a cipher text obtained from the encryption of the encryption block immediately prior to the encryption block to be encrypted to perform encryption processing.

16. (Original) The data processing method as set forth in claim 15, further comprising the step of managing the encrypted data stored in said storage means using a cluster containing one or more processing blocks and values initially used when encrypting an encryption block in one of said processing blocks.

17. (Original) The data processing method as set forth in claim 16, further comprising the steps of :

storing said one or more processing blocks at consecutive addresses of said storage means in the order of encryption;

storing said one or more encryption blocks in said processing blocks at consecutive addresses of said storage means in the order of encryption; and

storing said initial values at an address immediately prior to the address of at which the first encryption block in the cluster is stored.

18. (Original) The data processing method as set forth in claim 13, further comprising the step inserting data into said processing block to adjust the data length in the processing block so that the length of said processing block becomes a whole multiple of the predetermined data length of said encryption block.

6